APPENDIX D. EXAMPLE NUCLEAR CRITICALITY SAFETY ANALYSES

D.1 Double-contingency analyses. The purpose of this section is to provide an example of a double-contingency analysis of a potential criticality scenario to evaluate compliance with the Double-Contingency Principle (section 5.7.8). The main points of the illustration are

(a) identifying the potential criticality scenario (section 5.7.6),

(b) evaluating the scenario for compliance with the Double-Contingency Principle (section 5.7.8), and

(c) identifying the associated means of control (section 5.7.5).

Example # 1 below provides an involved scenario analysis with control reliability/failure evaluations for acceptability.

D.1.1 Example # 1. Assume that the quantity of fissile nuclide required for a particular operation is 2 kg of ^{239}Pu in oxide form that is greater than the minimum critical mass. On this basis, criticality protection is solely dependent upon excluding moderation from the area since geometry/volume is not controlled. Since nuclear criticality safety depends on the control of a single nuclear parameter, moderation, two separate and independent barriers need to be provided to prevent loss of moderation control. Thus, as shown in Figure D.1.1 (upper left-hand corner), nuclear criticality safety considerations require that moderating liquids be excluded from the dry processing location containing fissile material. Reviews of the design identified two credible sources of liquid to the dry location under operating conditions: (1) liquid backflow from an associated off-gas scrubber system, and (2) the unauthorized manual addition of liquids by operating personnel. Before proceeding, a brief description of the scrubber system is given below.

The off-gas scrubber system is provided to cool and scrub the off-gas coming from the dry location that contains fissile material in powder form (upper left-hand corner of Figure D.1.1). A vacuum is pulled on the system using a vacuum air jet located above the separator tank that is supplied by the high-pressure facility air system (90 psig). The off-gas first passes through the scrubber tank, where it mixes with liquid in the scrubber and forms a two-phase flow in the line to the separator tank. From the separator tank the off-gas goes to the vessel vent system. The liquid in the separator tank is circulated back (pumped) to the scrubber tank.

The design incorporates a jet bypass line leading to the vessel vent system (see Figure D.1.1). This bypass line contains an automatic valve (normally closed during operation of the jet) that is electrically interlocked to a high pressure switch. Also shown is a rupture disk located just off the separator tank. Note that for simplicity, Figure D.1.1 shows only those instrumentation and control features in the system that are referred to below.

D.1.1.1 Identifying potential criticality scenarios - logic diagram. In accordance with section 5.7.6, "Identifying Potential Criticality Scenarios," a logic diagram is constructed (see Figure D.1.2) as an aid to systematically identify the various scenarios that could lead to the accidental addition of liquid to the dry location, which is the mechanism for a potential criticality accident in this case. The logic diagram shows two credible liquid sources: Source 1 is liquid *coming from the scrubber* system; and

Source 2 is liquid from manual addition to the cabinet (operator error). Pursuing Source 1 (Figure D.1.2), three basic phenomena are identified: (1) back siphonage, (2) backflow resulting from a pumping action, and (3) backflow resulting from high pressure in the scrubber system. For the high-pressure case, two initiating events are identified: (1) eructation, and (2) pluggage of the air jet at the exit resulting in high pressure facility air (90 psig) applied to the scrubber system (Figure D.1.1). As shown in Figure D.1.2, back siphonage and eructation are judged to be incredible for this particular design and associated operating conditions. The pumping action case is identified in Figure D.1.2 as worthy of study, but it is not developed here (for simplicity). The potential criticality scenario designated for study below deals with pluggage of the air jet. This scenario is highlighted in Figure D.1.2 and may be summarized as follows:

> Potential criticality scenario - Mechanism: liquid addition to the dry location - Source: scrubber system liquid - Phenomenon: backflow due to high pressure in the scrubber system - Initiating event: pluggage of air jet at the exit.

D.1.1.2 Evaluation against the Double-Contingency Principle.

D.1.1.2.1 Identifying the two barriers for double-contingency. Simply stated, the Double-Contingency Principle says that two independent, controlled barriers should exist to prevent occurrence of a potential criticality accident scenario. The application of this principle is shown symbolically in Figure D.1.3, which is a duplicate of Figure D.1.2, with the two barriers added.

For this example, it is assumed that the two barriers chosen are (1) pressure relief via the jet bypass pressure/interlock system, and (2) pressure relief via the rupture disk. As illustrated in Figure D.1.4, with these barriers in place, this potential criticality scenario requires the occurrence of all of the following: (1) the initiating event - jet plugged at exit, (2) the failure of Barrier 1 - failure to relieve pressure via the jet bypass pressure/interlock system), and (3) the failure of Barrier 2 - failure to relieve pressure via the rupture disk.

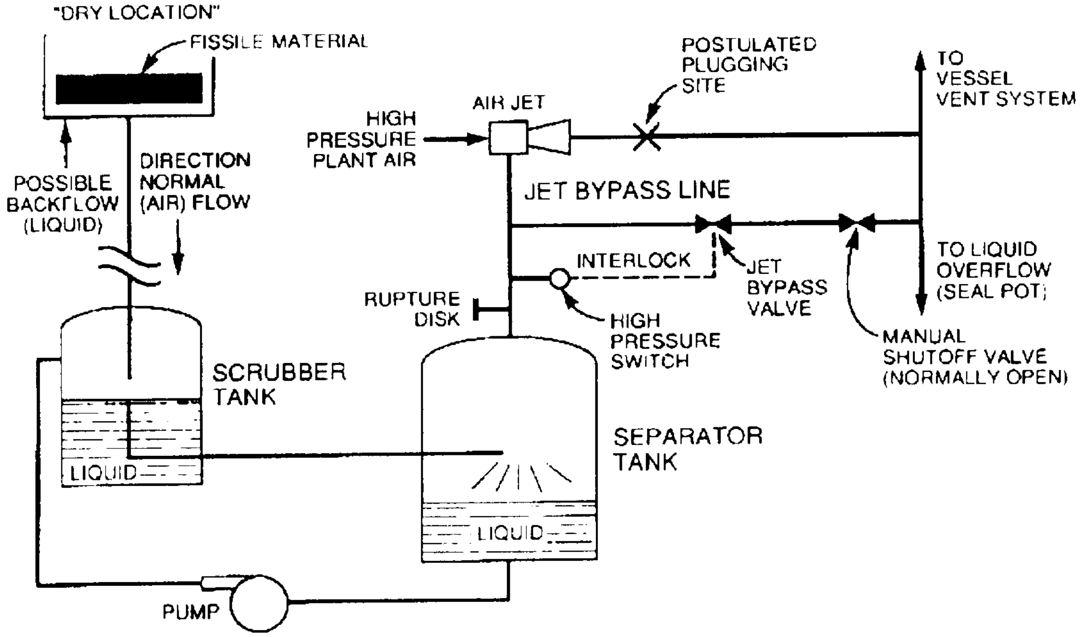

Figure D.1.1. Schematic of dry location and scrubber system.

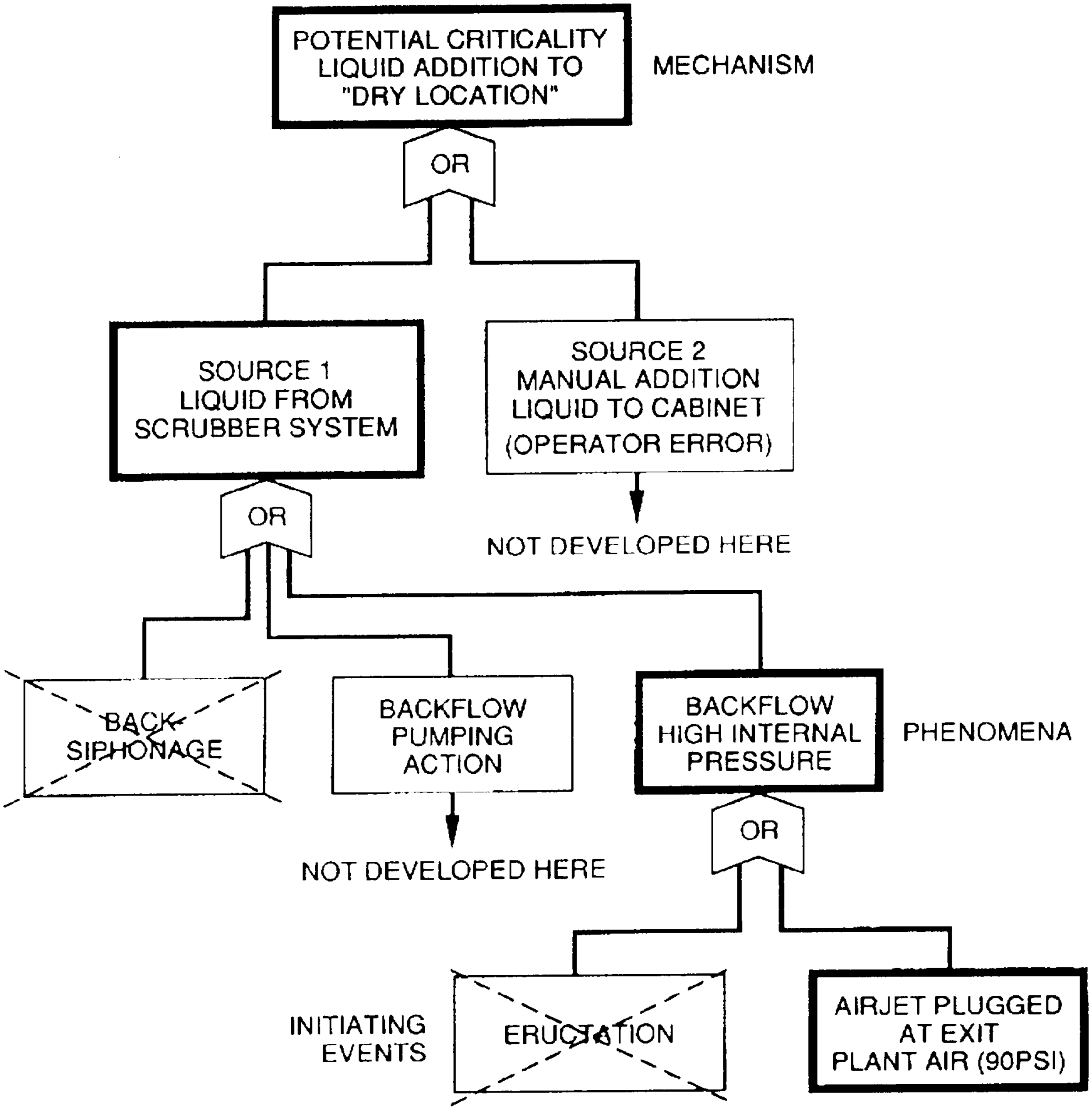

Figure D.1.2. Logic diagram for potential criticality via liquid addition to dry location.

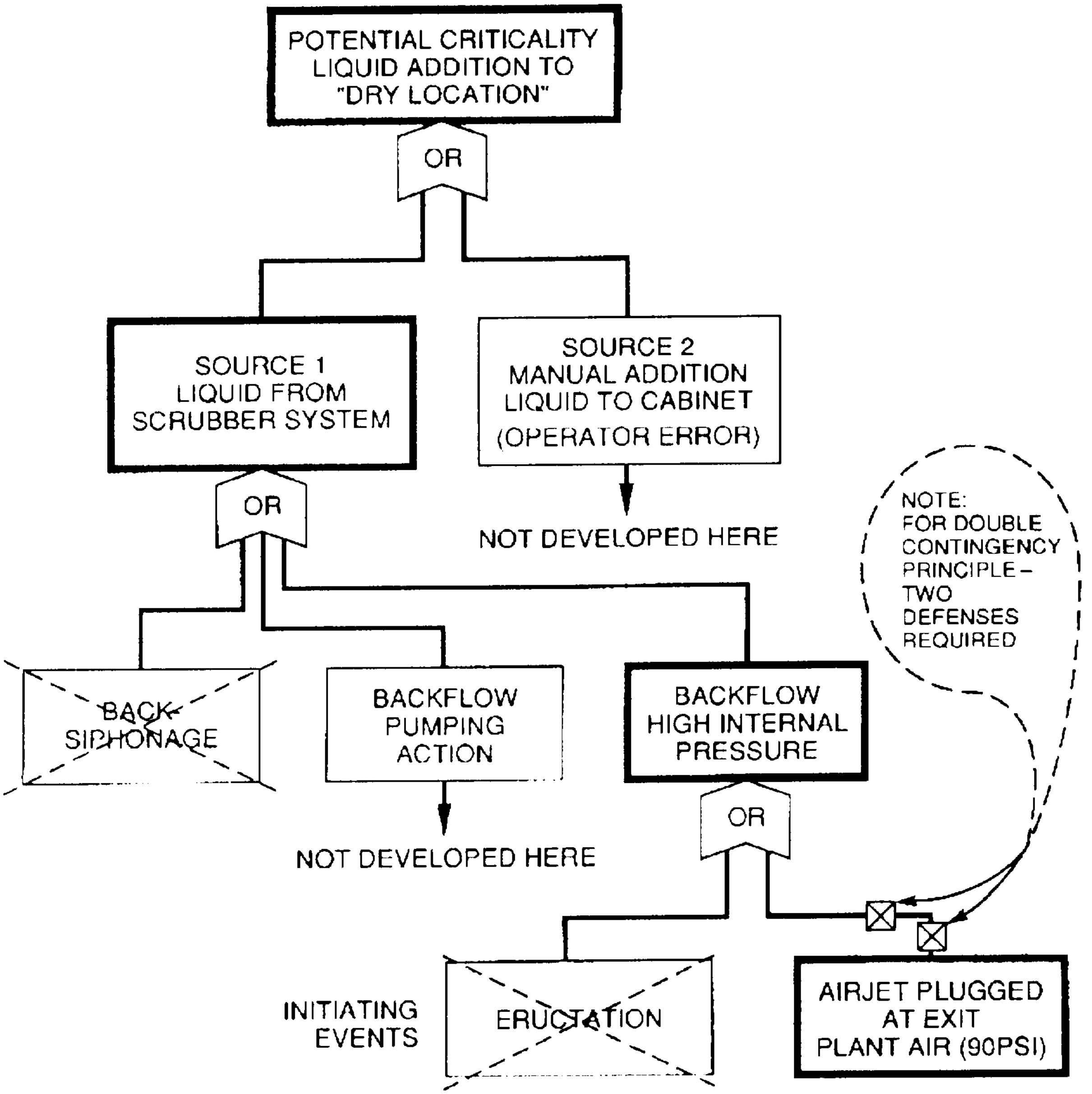

Figure D.1.3. Logic diagram for potential criticality via liquid addition to dry location - two barriers added.

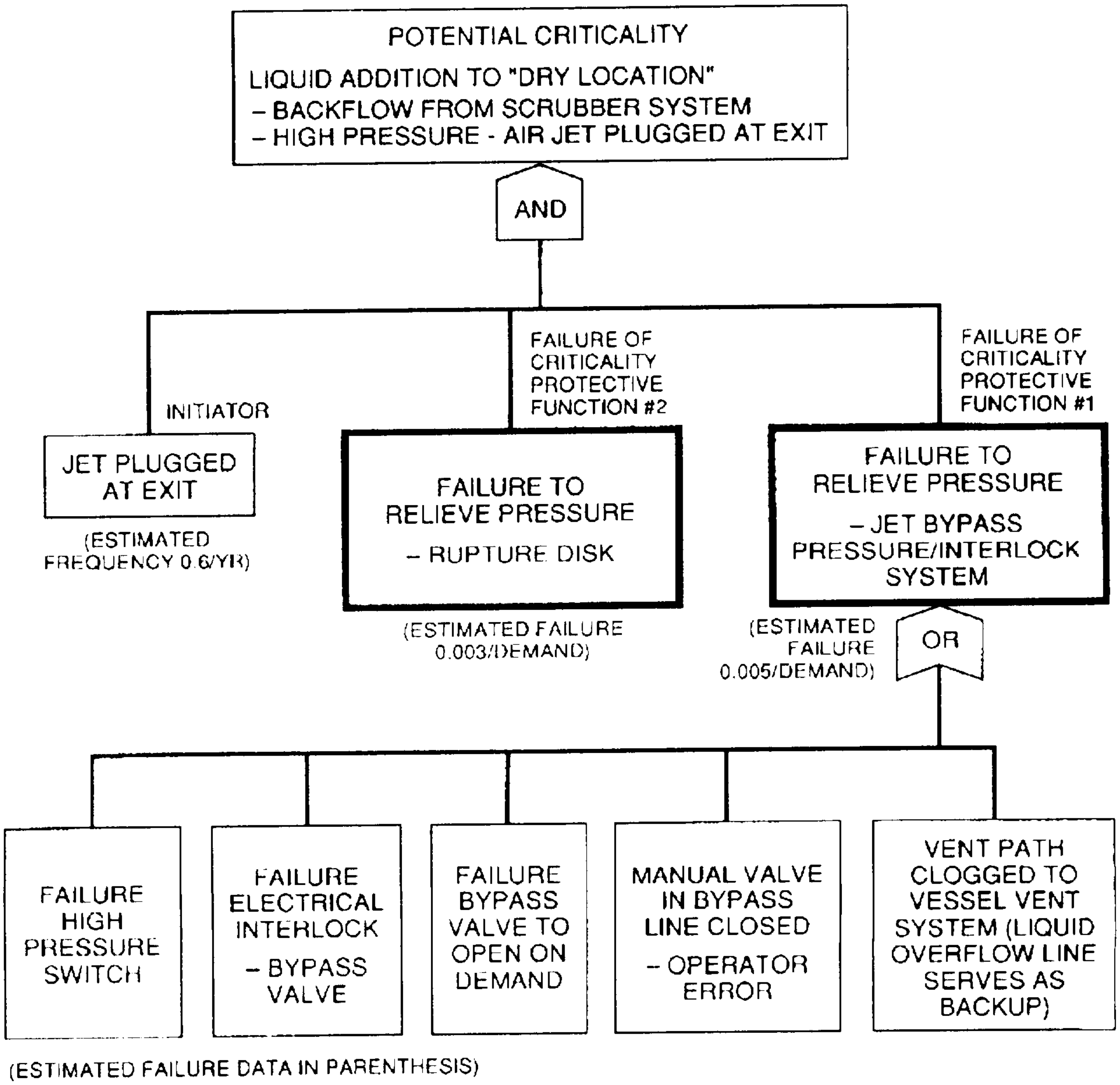
POTENTIAL CRITICALITY
LIQUID ADDITION TO "DRY LOCATION"
– BACKFLOW FROM SCRUBBER SYSTEM
– HIGH PRESSURE - AIR JET PLUGGED AT EXIT
AND
INITIATOR
FAILURE OF CRITICALITY PROTECTIVE FUNCTION #2
FAILURE OF CRITICALITY PROTECTIVE FUNCTION #1
JET PLUGGED AT EXIT
(ESTIMATED FREQUENCY 0.6/YR)
FAILURE TO RELIEVE PRESSURE – RUPTURE DISK
(ESTIMATED FAILURE 0.003/DEMAND)
FAILURE TO RELIEVE PRESSURE – JET BYPASS PRESSURE/INTERLOCK SYSTEM
(ESTIMATED FAILURE 0.005/DEMAND)
OR
FAILURE HIGH PRESSURE SWITCH
FAILURE ELECTRICAL INTERLOCK – BYPASS VALVE
FAILURE BYPASS VALVE TO OPEN ON DEMAND
MANUAL VALVE IN BYPASS LINE CLOSED – OPERATOR ERROR
VENT PATH CLOGGED TO VESSEL VENT SYSTEM (LIQUID OVERFLOW LINE SERVES AS BACKUP)
(ESTIMATED FAILURE DATA IN PARENTHESIS)

Figure D.1.4. Contingency analysis diagram.

D.1.1.2.2 Qualification of the barriers for double-contingency

As discussed in section 5.7.8, it is important that the failure of a barrier for double-contingency be an unlikely event. The determination of whether a failure of a barrier for double-contingency is unlikely may be made on the basis of engineering judgment or failure rate data, if available. For this example, assume that failure rate data are available. In accordance with section 5.7.8.3, the guidelines for acceptability when quantitative data are available are: (1) Guideline 1 - the estimated probability that the barrier will fail is no greater than once in 100 demands or 0.01/demand, and (2) Guideline 2 - the product of {the estimated frequency of the initiating event} times {the estimated probability of failure of the barrier - as applied in Rule 1} is not greater than once in 10 years or 0.1/year.

Guideline 1 - As shown in Figure D.1.4 and Table D.1.1, the probability that Barrier 1 will fail upon demand is estimated at 0.005/demand, thus meeting the 0.01/demand guideline. Correspondingly, the failure probability of Barrier 2 is estimated at 0.003/demand, which is better than the 0.01/demand guideline.

Both barriers are judged to meet Guideline 2. The frequency of the initiating event -- pluggage of the air jet at the exit during operation -- is estimated (conservatively) to be in the vicinity of once every twenty months (based on previous experience with similar equipment and operating conditions). Therefore, the frequency is shown as 0.6/year (Figure D.1.4 and Table D.1).

For Barrier 1: (estimated frequency of the initiating event) times (estimated probability of failure of Barrier 1) = 0.6/year × 0.005/demand = 0.003/year, thus meeting the 0.1/year guideline.

For Barrier 2: (estimated frequency of the initiating event) times (estimated probability of failure of Barrier 2) = 0.6/year × 0.003/demand = 0.0018/year, thus meeting the 0.1/year guideline.

Note: As a point of interest, in this example the estimated frequency for this potential criticality scenario (based solely on the three factors discussed above) is:
$0.6/\text{year} \times 0.005 \times 0.003 = 9 \times 10^{-6}/\text{year}$,
that is a recurrence interval of approximately 111,000 years.

Independency of barriers. The two barriers in this example are judged to be sufficiently independent. On the negative side, both barriers involve the sensing of a common process parameter, high pressure, and both have the same basic function, which is to relieve pressure. However, on the positive side the two barriers do not share components, and they operate quite differently -- not likely to be subject to common-cause errors during facility operations such that both systems would be inadvertently taken out of service, or in maintenance operations such that common calibration or set-point errors might occur.

D.1.1.3 Identifying the means of control for each contingency barrier. As discussed in section 5.7.8.4, the prominent identification of the means of control associated with a barrier for double-contingency is important. Special care should be exercised to maintain these controls during facility operation, maintenance activities, and subsequent design changes. As shown in Figure D.1.4 and Table D.1.1, five controls are associated with Barrier 1 (see bottom of Figure D.1.4). The failure of any one of these could defeat the barrier. Three of the five are hardware items. They are the sensor, the electrical interlock, and the automatic valve. All three will require administrative controls in the form of functional testing and preventive maintenance to maintain high reliability. The other two controls (of these five) will require special procedural controls (such as verification that the manual valve in the bypass line is OPEN prior to operating the air jet). Only one means of control is associated with Barrier 2, that is, the rupture disk itself).

D.1.1.4 Review, relative to the other nuclear criticality safety objectives. The last step in the double-contingency analysis is to reflect back on the design relative to all six of the basic design objectives discussed in section 5.7.4, particularly the following two objectives.

> Objective 3: Is there a feasible design alternative that will completely eliminate this potential criticality scenario? In this example the possibilities may include design alternatives to (1) eliminate the use of liquids in the auxiliary systems to the dry location (probably not practical here), or (2) eliminate the 90-psig motive force (in favor of an alternative).

> Objective 1: If feasible, have the preferred methods been incorporated? For example, the use of geometry control in the dry location (if feasible) could eliminate the necessity of precluding liquids from the dry location for reasons of nuclear criticality safety.

Table D.1.1. Contingency Analysis - Summary Sheet

STATEMENT OF CRITICALITY SCENARIO

Specific Location: Dry Location
Mechanism: Liquid addition to dry location
Source: Scrubber system liquid
Phenomenon: Backflow due to high pressure in scrubber system
Initiating Event: Pluggage of air jet at exit.

INITIATING EVENT Pluggage of air jet at exit - estimated frequency, approx. 0.6/year

BARRIER 1

DESCRIPTION: Relieve (high, abnormal) pressure via jet bypass pressure/interlock system.

QUALIFICATION OF BARRIER 1:
Guideline 1: Estimated Probability of barrier failure - 0.005/demand.
Guideline 2: Product of (est. freq. of initiating event) times barrier failure prob. = 0.6/year × 0.005 = 0.003/year.

LIST OF ASSOCIATED MEANS OF CONTROL:

1. High-pressure switch - separator tank (open jet bypass valve at >4 psig).
2. Electrical interlock - interlocks pressure switch to automatic valve in jet bypass line to OPEN on demand.
3. Jet bypass valve (automatic) in jet bypass line.
4. Manual valve in jet bypass line - requires administrative controls to ensure valve open.
5. Vent line to vessel vent system - requires administrative control to ensure/verify that line is free. (Note: liquid overflow line to serve as backup.)

BARRIER 2

DESCRIPTION: Relieve (high, abnormal) pressure via the rupture disk on separator tank.

QUALIFICATION OF BARRIER 2:
Guideline 1: Estimated Probability of barrier failure - 0.003/demand
Guideline 2: Product of (est. freq. of initiating event) times barrier failure prob. = 0.6/year × 0.003 = 0.0018/year.

LIST OF ASSOCIATED MEANS OF CONTROL

1. Rupture disk on separator tank (rupture pressure >6 psig)

D.2 Examples of eliminating unnecessary criticality scenarios. Rather than accepting an element of risk, it is preferred that the risk be removed entirely, if feasible. As discussed in section 5.7.7, an effort should be made to explore the feasibility of design changes aimed at eliminating potential criticality scenarios. The three examples below are intended to illustrate the intent and lines of inquiry.

D.2.1 Example # 1 - Removing a potential water source to a dry area. A design concept incorporates a water-cooled heat exchanger to cool the off-gas from a process. Evaluations reveal a potential criticality scenario that begins with cooling water leaking across the tubes of the heat exchanger (the initiating event), followed by the loss of detection and protective measures, and ending with water reaching a location that must remain dry for nuclear criticality safety.

Before accepting this risk, consideration should be given to the feasibility of alternative cooling means that will completely eliminate this scenario. For example, it may be feasible to provide the off-gas cooling function using a design that does not involve water, such as with an air-cooled or freon-cooled design. Using an alternative cooling method, the potential source of water to the dry location is entirely eliminated.

D.2.2 Example # 2 - Eliminating the motive force. A design concept incorporates an air jet connected to a process vessel to be used for the vacuum transfer of liquids into a vessel. The air jet is supplied by a high-pressure facility air system. Evaluations show a potential criticality scenario starting with pluggage of the exit to the jet with trash or other material, which produces a high positive pressure in the process vessel. In turn, the high pressure provides a motive force causing liquid in the vessel (containing fissile nuclides) to accidentally backflow through interconnecting piping and reach locations that are unsafe for criticality, such as instrument air systems, cold feed tanks, and ventilation systems.

In such a case, the feasibility of alternative design concepts, such as an electrically driven pump or alternative system, should be explored that, while retaining the solution transfer capability, have no potential for producing large positive pressures on the vessel contents.

D.2.3 Example # 3 - Eliminating the potential for over-concentration. A design concept incorporates an evaporator for concentrating aqueous solutions containing fissionable material product. Nuclear criticality safety of the evaporator is based on limiting the concentration of the fissionable material product to a safe value. An automatic control system is used to regulate the specific gravity of the concentrate. (The specific gravity can be directly correlated to product concentration levels.) Backup protection against product over-concentration is achieved using active protective devices (sensors and interlocks) that shut off the steam supply to the evaporator when the specific gravity of the concentrate approaches the limit for nuclear criticality safety. A potential criticality scenario is identified that begins with the loss of specific gravity control, followed by failure of the active protective devices to shut off the steam supply, and resulting in high product concentration levels exceeding the nuclear criticality safety limits.

In this case, design considerations should be given to identifying a feasible means to eliminate the possibility of product over-concentration. For example, the circumstances may permit using a value for the steam supply pressure to the evaporator that is high enough to achieve the normal product concentration level but low enough to thermodynamically preclude the evaporator system from being capable of attaining the higher product concentration levels associated with nuclear criticality safety concerns. With this approach, a criticality accident due to product over-concentration is not possible, regardless of the proper performance of the control and protective devices.

D.3 Examples of passive-engineered features and devices. The purpose of this section is to provide examples of the group of controls called passive-engineered features and devices, that are discussed in section 5.7.5.1.1. This group consists of fixed, passive design features and devices with no moving parts. No electrical, mechanical, or hydraulic action is required. In many cases, these features and devices are employed to protect against the unwanted transport of liquids from favorable to unfavorable locations.

D.3.1 Air break. An air break is a simple, highly reliable means for backflow or back siphonage prevention with virtually no failure mechanisms. With this device, an air gap is created by interrupting a piping system. This device is illustrated in Figure D.3.1 and is applicable to situations where line pressure may be broken. Note that such a device would rank very high as a preferred control for nuclear criticality safety considering reliability, range of coverage, and operational support requirements. Regarding range of coverage, this device provides direct, positive protection against backflow to the feed tank in Figure D.3.1 -- independent of the reason for the backflow. For these reasons, the air break should be employed as standard practice, whenever applicable.

D.3.2 Barometric seal leg. Figure D.3.2 illustrates the use of barometric seal leg connections, or gooseneck connections, when there are multiple-source line connections to a main header. Here, a gooseneck connection is used for each source connected to the header. The arrangement shown in Figure D.3.2 includes overflow capability from the header and acts to prevent liquid that has arrived to the header (from one line source) from back-flowing through other line source connections. Of course, undetected pluggage of the overflow line could defeat the safety function. Because of its simplicity and effectiveness, this arrangement should be incorporated whenever backflow from a header through a source line could introduce nuclear criticality safety concerns.

D.3.3 Criticality drain. A criticality drain is a device that normally serves both radiological and criticality safety functions while preventing liquid buildup in moderation controlled enclosures such as gloveboxes. Figure D.3.3 illustrates the use of a J-trap type criticality drain. The portion of the drain inside the glovebox is raised slightly above the bottom and has a baffle to prevent clogging (some types use screen mesh stand-offs). Thus, the maximum credible depth of liquid in the glovebox is a fraction of minimum critical thickness. The portion of the device below the glovebox is partially filled with an oil selected for its low evaporation rate and resistance to combustion. This oil forms a radiological seal, and this region of the device may be transparent or have a level indicator and fill port. The end of the J-trap may be open or connected to vented drain piping based upon radiological considerations. In the event of a spill or leak exceeding the inside lip height, liquids pass through the trap. The J-trap and any connecting piping are large enough in diameter to accommodate the maximum credible flow rate into the glovebox. If the drain(s) are piped to receiver vessel(s), they shall be criticality-safe and equipped with overflow lines to avoid backups.

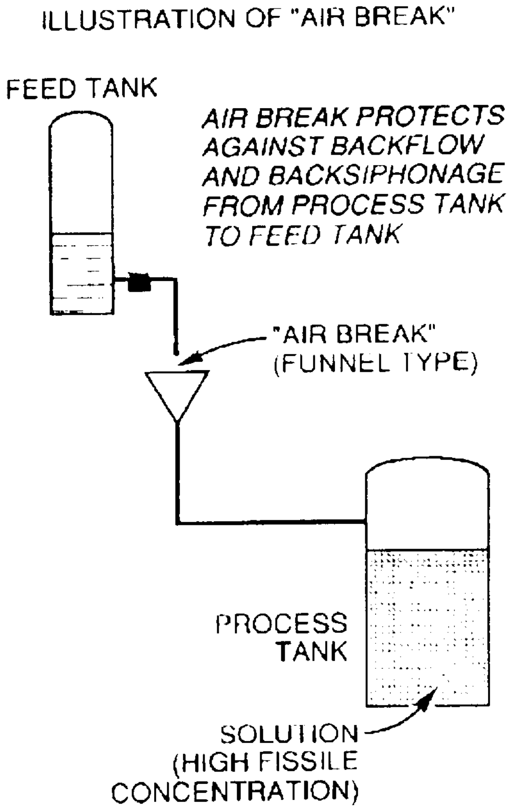
ILLUSTRATION OF "AIR BREAK"
FEED TANK
AIR BREAK PROTECTS AGAINST BACKFLOW AND BACKSIPHONAGE FROM PROCESS TANK TO FEED TANK
"AIR BREAK" (FUNNEL TYPE)
PROCESS TANK
SOLUTION (HIGH FISSILE CONCENTRATION)

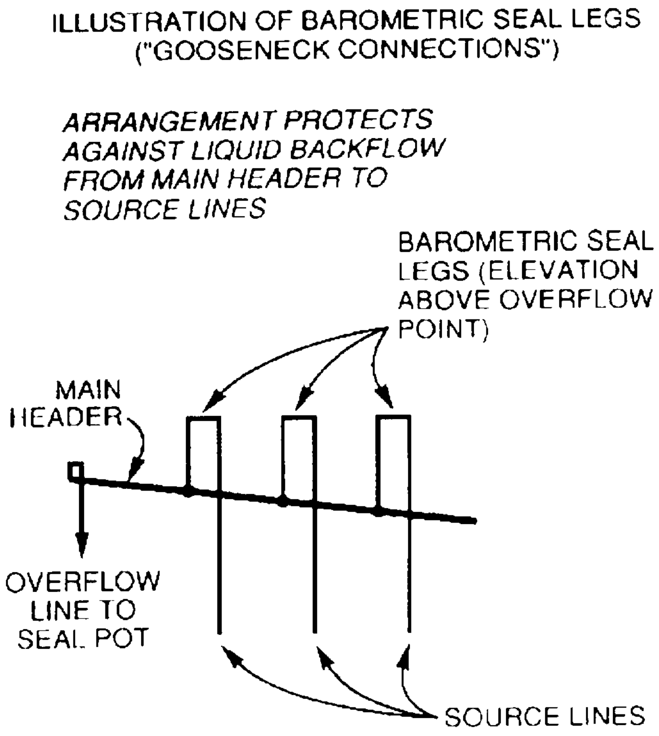
ILLUSTRATION OF BAROMETRIC SEAL LEGS ("GOOSENECK CONNECTIONS")
ARRANGEMENT PROTECTS AGAINST LIQUID BACKFLOW FROM MAIN HEADER TO SOURCE LINES
BAROMETRIC SEAL LEGS (ELEVATION ABOVE OVERFLOW POINT)
MAIN HEADER
OVERFLOW LINE TO SEAL POT
SOURCE LINES

Figure D.3.1. Schematic of air break.

Figure D.3.2. Illustration of barometric seal.

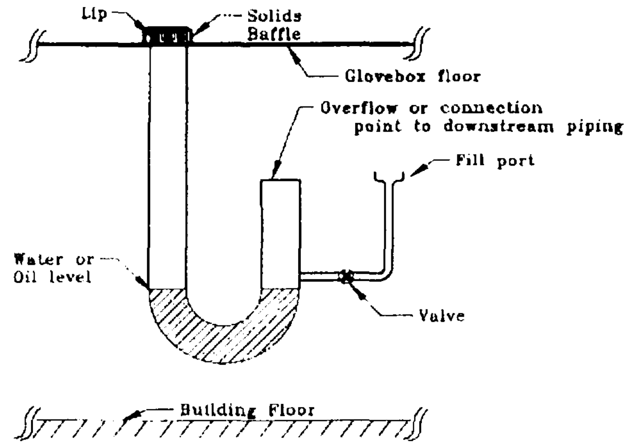

Figure D.3.3. Criticality Drain.

D.3.4 Nuclear safety blank. A nuclear safety blank is a simple, positive means for preventing the accidental transfer of liquid through a line to an unsafe location. This blank typically consists of a flat, solid metal disk inserted in a pipe flange to block the flow of liquid in special circumstances, such as special processing campaigns, where the accidental transfer of liquid through the line to another location could lead to criticality concerns. The device should be designed to make unplanned removal mechanically difficult and labeled for easy identification in the field. A spectacle flange is a nuclear safety blank combined with a second disk with flow hole(s) and resembles a pair of eyeglasses. This design provides flexibility while having the advantage of providing positive proof that flow is blocked if the disk with the hole(s) is visible. However, all nuclear safety blanks should be leak tested and surveyed for wear and corrosion at start-up and at appropriate intervals. With suitable administrative controls to guard against unplanned removal, these devices would likely qualify as a double-contingency control, whereas administrative controls to keep a block valve in the closed position would not qualify.

D.3.5 Large line sizes. Under certain conditions, the pluggage of a line can cause the unplanned redirection of liquid to an unsafe location. By selecting a large, but safe, line-size larger than would otherwise be employed, it may be possible to make pluggage of the line considerably less likely to occur than would otherwise be the case.

D.3.6 Restricting orifices. Under certain conditions, the occurrence of an abnormally high flow rate in a line can lead to a criticality concern. In such a case, a restricting orifice in the line can provide a simple, reliable means of protection.

D.3.7 Relative elevation. The relative elevations of various equipment items and piping in a facility can be an important consideration in determining the potential for the unplanned transport of liquid from safe to unsafe locations. For example, simple leakage past a block valve can result in the unplanned flow of liquid (by gravity) from a source tank to a receiving tank located at a lower elevation. This mode of unplanned transport (by gravity) can be eliminated in the design concept by reversing the respective elevations of the two tanks.

These examples serve to illustrate the importance of clear identification of those design features and controls important to nuclear criticality safety. Many of the design features and devices in this group, such as a restricting orifice or size of a line, are not normally associated with nuclear criticality safety, and in the absence of clear identification, their importance to nuclear criticality safety may be overlooked.

D.4 Examples of active protective devices. The group of controls identified as active protective devices is discussed in section 5.7.5.1.2. These devices are characterized as add-on devices involving moving parts, are designed to act upon demand, or are sensing devices. Many such devices are electrical/mechanical. The first two examples below illustrate devices in this group that are strictly mechanical (preferred to complex electro-mechanical systems unless there is a demonstrable benefit from additional complexity).

D.4.1 Rupture disk. Phenomena causing abnormally high pressure in a vessel can cause the unwanted flow of liquid in the vessel to unsafe locations, as illustrated in the example in section D.1.1. The normal engineering function of a rupture disk is to protect the vessel itself from over-pressurization. However, it may be feasible in a given situation to select a lower pressure rating for the rupture disk (than would otherwise be needed) to limit maximum pressures in a vessel below the values required to transfer the liquid to an unsafe location. Assuming that adequate reliability of this device can be established, the rupture disk would serve a valuable nuclear safety function in addition to its vessel protective function.

D.4.2 Backflow prevention devices. As discussed in section D.3, an air break provides very effective protection against backflow and back siphonage. However, there are situations where an air break device is not suitable, since line pressure would be lost. When it is necessary to maintain line pressure, an in-line device may be considered. A review of the various backflow and back siphonage prevention designs could include: (1) single check-valve design, (2) double check-valve design, (3) double check-valve design with vent, (4) reduced-pressure device, and (5) reduced-pressure device with internal air gap. This spectrum of design types serves to illustrate the general notion involved in selecting a double-contingency means of control. Due to questions of seal integrity, it is likely that most of these backflow prevention devices would be determined to have insufficient reliability to qualify as a double-contingency means of control. On the other hand, one or more of these designs may so qualify, depending on unique design features and the service conditions involved.

D.4.3 Radiation monitoring systems. A radiation detector, readout, alarm, and associated motor- or air-operated valve(s) that close(s) on a dose rate set point is a relatively simple active protection system for either radiological safety, criticality safety, or both. Such systems may be portable or fixed. They can be conservatively used for criticality safety of geometrically unfavorable tanks by assuming that all radioactivity is due to the presence of fissionable nuclides. More sophisticated applications use gamma spectrum analyzers to more accurately estimate fissionable material content. In-line detectors should be close to the lower side of piping at strategic points to maximize detecting solids-buildup that sampling may miss, and detectors on tanks should be located near places where solids-buildup is most likely. A variant of this system is a soluble neutron poison monitoring system where increasing neutron flux means poison concentration is decreasing. However, these detectors should not be located under pipes or tanks because poison can precipitate and skew results. Regardless of the specific application, it is important to design, operate, and maintain such systems to avoid frequent false alarms and thus create a distrust of instrument readings and alarms.